



DIGITAL RIGHTS, DIGITAL WRONGS

Simon Williams looks at Digital Rights Management technology and asks whether efforts to stamp out piracy are riding roughshod over consumers' rights

One huge benefit of digital content – be it music, video or software – is that it's easy to make perfect copies to order. But for the record companies, film producers and software houses whose profits depend on intellectual property, this ease of copying is both a blessing and a curse. To combat piracy they need to control who copies content and how often. They also like to control what people do with their content.

In this feature we look at the Digital Rights Management (DRM) technology they use to do this, and how it affects legitimate consumers. If you've paid for a piece of music or a film, you expect certain rights. Many of us feel we should be able to copy a CD to MP3 or a DVD to DivX, to play on portable or car-based media players. Is the new technology tipping the balance too far towards the film studios and music companies?

WHAT IS DRM?

It is hard to stop people duplicating digital files, and much content has no copy-protection at all. Most music and software can be duplicated by simply ripping to an MP3 file, copying a CD or burning a DVD. File-sharing services on the internet make it very simple to obtain pirated

software. Piracy costs the UK film and music industries £818 million a year, according to the Federation Against Copyright Theft (FACT). With this much money at stake, copy protection has become a priority for all content providers – and a hotbed of technical innovation.

There are several different approaches to copy protection. The simplest way to keep tabs on copying is to require that content is registered before use. This is just about practical for software, but not for music or DVDs. A second approach is to try and prevent PC-based copying by technical means. Engineers have successfully exploited differences in the way domestic CD players and PC drives work to create CDs that play in domestic players but not PCs. They have also used various peculiarities of how CDs and DVDs work to inject data into discs that can't be ripped or copied. Games discs are particularly difficult to copy perfectly due to such schemes.

DRM is more sophisticated than either of these approaches. Typically, a DRM scheme encrypts the content then relies on the player or PC to police access to it. This requires a player smart enough to check what rights the user has to the content and powerful enough to decrypt it on the fly. DVDs use content encrypted using the

CSS system, and manufacturers of players have to obtain a key so their hardware can decrypt the content. This licence system was designed to give the DVD Copy Control Association – the organisation that distributed the keys – a degree of control over devices and software designed to read DVDs. However, CSS encryption was cracked back in 1999. This made DVD software development a free-for-all, and ripping and copying software soon became widespread.

For DRM to work it's also important that the player can't be compromised. DVD players were supposed to prevent you viewing DVDs made in other parts of the world. However, this control has proved ineffective because players were designed to be firmware upgradeable, and new firmware can remove the region control.

THANK YOU FOR THE MUSIC

DVD copy protection may have been a failure, but today's technology is far more effective. iTunes and the new, legal Napster use advanced DRM to control what you can do with music you download. Downloaded tracks from such music sites can be played on the receiving computer, copied to a music player and burnt to a CD. However, there may be restrictions on the



number of CD copies you can make and there may also be restrictions on downloading the same track again if you lose it. Most download sites allow three separate downloads of the track you've paid for. The table (right) shows what iTunes, Napster, MSN Music and My Coke Music allow you to do with your music.

The table also covers the second way of obtaining music from the internet. Many sites offer a streaming service for a fixed monthly fee. Under these systems, you can listen to your selection of music directly from the music website, but have no right to save it on your PC or transfer it to a music player.

With the increasing availability of broadband, this kind of streaming service is becoming more popular. Many users liken it to listening to a radio, and perhaps that's why most people accept that when their subscription lapses, their access to music stops.

HOW MUSIC DRM WORKS

Most online services use Microsoft's Secure WMA format, which is protected by Microsoft's DRM 10 system. The same DRM is used in the WMV format to secure video files. Microsoft's DRM goes beyond simple copy-protection, making it suitable for subscription services as well as selling digital media by download.

Secure WMA audio files are encrypted and don't include the 128-bit keys within them. Keys are provided separately by the service provider (MSN, Napster or whoever) as part of the licence, which is also encrypted. The licences are stored separately on your computer and can be accessed by any approved software player, such as Windows Media Player, when a file is played. The DRM software then checks that all the components involved in playback, such as the audio drivers, are certified with digital certificates and haven't been compromised. This makes Secure WMA files nearly impossible to rip to an unprotected format such as MP3.

The digital rights you have to the content are stored in the licence file. These are almost always restrictions on use, and may include start and end dates, the number of allowed plays, restrictions on transfer to media players and on burning content to CD or DVD. These rights are recorded within the encrypted licence, not the media file, and may be changed or revoked.

The licence itself is divided into two parts: a 'root' licence, which includes information such as the expiration date of playing rights, and a series of 'leaf' licences, which contain rights specific to each audio file. This gives content services that offer subscriptions the ability to update a small number of root licences, rather than what may be hundreds or thousands of individual media track licences.

Licences are tied to specific PCs by a signature based on the PC's component parts. This means that shifting both the WMA file and the licence to another PC won't give access to it; a separate licence must be obtained for the new PC. This means you can't sell on a secure WMA file – they're non-transferable. Any player you use to play downloaded secure WMAs on the move will be tied to a specific PC, so it can't take files from other computers, either.

COMPATIBILITY PROBLEMS

At first glance, downloading an album doesn't involve restrictions too onerous compared to buying a music CD. Most people won't be

DRM ON MUSIC DOWNLOAD SITES

	iTunes	Napster	MSN Music	My Coke Music
Cost streaming/download	No streaming, 79p/track	£9.95/month or 79p/track	£5.99/month or 75p/track	No streaming, 80p/track
Computer type	Mac or PC	PC only	PC only	PC only
Software used	iTunes	Napster	Windows Media Player	Music Manager
DRM used	ACC	Secure WMA	Secure WMA	Secure WMA
Number of plays	Unlimited	Unlimited	Unlimited	Unlimited
Burn to CD?	At 79p/track	Only after download at 79p/track	Only after download at 75p/track	At 80p/track
Players supported	iPod, all types	Over 75, inc Creative, Rio, iRiver	Over 60, inc Archos, iRiver Creative, Rio	Over 60, inc Archos, iRiver, Creative, Rio
No. of downloads per track	Up to five	Up to three	Up to three	Up to three

prevented from doing the kind of things they want to do with the music they've bought.

However, it's easy to rip CD tracks to MP3 files that can be carried around on a portable player of your choosing. With downloaded tracks this gets a lot more complicated, not least because there are several rival DRMs. ACC, the format used by Apple for iTunes, is not the same as that offered by Microsoft in Secure WMA. These proprietary schemes tie customers to particular software and music players. Music downloaded from iTunes won't play through Windows Media Player, but has to be run from Apple's own iTunes software and can be played only on iPod music players.

While secure WMA files are a bit more flexible, there are still many portable music players that can't handle them, because they don't support DRM 10. Microsoft's Plays For Sure scheme is designed to give people more confidence when buying media players or music from internet sources that the media they download will be compatible with their hardware. In the case of media players such as those from Creative, iRiver and Archos, it means that the players themselves have been tested as secure and capable of running Microsoft DRM. Don't expect to be able to play WMAs on an iPod any time soon, though.

LAISSEZ FAIR

In at least one country, platform-specific DRM systems such as these are considered unfair practice. France intends on insisting that each download service operating within its borders

provides music that can be played on any portable player. Apple, which currently holds around 70 per cent of the French music download market, is considering whether to comply with the new law, should it finish its passage through the French Senate, or pull out of the French market altogether.

If the French act becomes law, it could encourage other countries to follow the example and we could see the removal of these software-to-hardware ties in the UK, too. Traditionally, though, the corporate lobby in this country is more powerful than consumer protests.

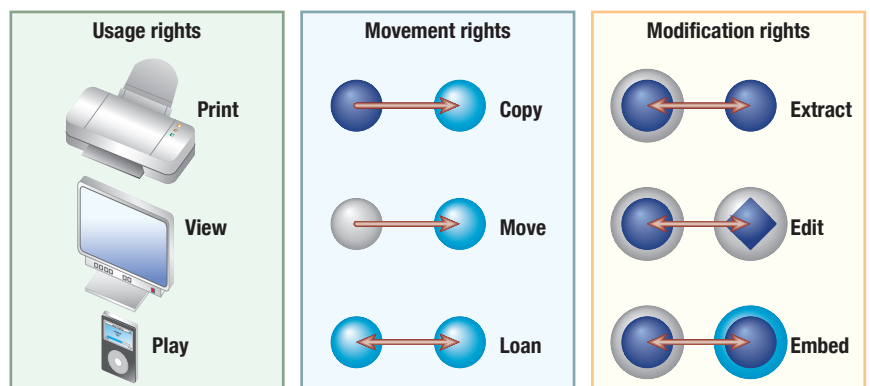
There's one clear benefit of DRM to consumers. It's extremely convenient to be able to download music as and when you want. It's easy to see how this kind of model for hiring and buying music can be extended to other media, the most obvious being video. As broadband speeds continue to increase and more people have access to fast downloads or streams, DRM could make internet movie rentals common.

PROTECTING SOFTWARE

Software copy-protection is getting more sophisticated, too. Software houses obviously want to combat piracy, but DRM also promises to let them sell their software in different ways. Microsoft and other software suppliers have long been interested in the idea of renting their products rather than selling them, because it ensures a regular income stream and in the long term this income could be increased.

Microsoft's Product Activation, as used on Windows XP and several other Microsoft

Types of digital rights



DRM restricts what you can do with media. At the simplest level, you'll want to show it on a screen, print it out or play it. At the next level, you may want to move it to a different player, copy it from one playing device to another or loan it to someone else. Finally, you may want rights to make alterations, such as copying it into a compilation or sampling it to incorporate it in original work of your own.



products, is a step in this direction. Product Activation ties a product to a specific PC. It does this by calculating a unique 'fingerprint' for your PC based on the hardware present.

The graphics card, SCSI adaptor, IDE adaptor, network adaptor, MAC address, RAM size, processor type, processor serial number, hard disk and its volume serial number, CD/DVD drive and whether the computer is dockable (ie a notebook) all contribute to the equation – called a hash function – used to calculate the fingerprint.

When activation takes place, a digital certificate around 9KB in size is created on the PC. Thereafter regular checks make sure the software is still running on the same PC. According to Microsoft, you can make substantial changes to the configuration of your PC – by changing the motherboard and processor, swapping the graphics card, adding a hard disk or replacing the CD drive, for example – before re-activation would be necessary.

Microsoft already rents some of its software to companies that rent PCs or run internet cafés. It will also rent you Windows and Office software under its Open Value Licence if you're running five or more PCs. At the moment, Microsoft trusts you to remove the software when the rental lapses, but in theory, a DRM licence tied to a PC using Product Activation could be used to enforce this.

NEXT-GENERATION DRM

The latest big challenge for DRM is next-generation DVDs. Both Blu-ray and its rival HD DVD have chosen the Advanced Access Content System (AACS) to protect the contents of their 30GB-plus DVDs.

AACS has been co-developed by several of the big names in content creation, including Microsoft, Walt Disney and Warner Bros. It's designed to control what you can do with the media it's protecting. For example, AACS should enable authorised copying of a movie to, say, a home media server, while preventing the same movie being copied to a second disc.

AACS encrypts content so that only licensed hardware and software can read the discs. This is similar to DVD's CSS system, but the AES encryption is stronger, and AACS provides a facility for content owners – music companies, film corporations and software providers – to revoke permission to play at any time.

It does this using Media Key Block technology, part of the mechanism that supplies

the key for decryption of the disc. A set of keys is included on each disc, allowing it to play on approved players. But if a particular player is 'compromised', discs can be produced with the keys for that 'barred' model so the discs won't play on that type of player. This means that if a rogue company produced a software or hardware player that could copy discs, the content providers could stop that player from reading the discs at all.

While AACS is the main protection scheme for HD DVD, Blu-ray offers two additional systems, BD+ and ROM Mark, which could explain its popularity with big content providers such as 20th Century Fox.

BD+ can dynamically update the DRM firmware in a Blu-ray player to counteract attempts to reprogram the drive. This should prevent firmware patching, such as removing region control. ROM Mark is a unique, undetectable identifier that would be applied to each Blu-ray disc, specific to the

machine that presses it. The mark is positioned at a set place on the disc and has a unique code. It's said to be invisible to a consumer playing a disc on a commercial player, but will make any copies of the disc unplayable. Customs officers or other enforcement agencies will be able to use a specially modified player to read the code and compare it with legitimate codes to determine if discs are authentic.

FURTHER READING

Microsoft DRM 10
www.microsoft.com/windows/windowsmedia/forpros/drm/faq.aspx

AACS white paper
www.aacsla.com

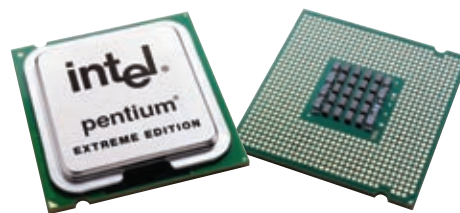
Microsoft Product Activation
www.microsoft.com/technet/prodtechnol/winxp/pro/evaluate/xpactiv.msp

DEEP DRM

In the past, hackers have often defeated copy-protection by undermining the software that manages the system. At one time, it was common practice for hackers to copy games by using a different operating system from the one the copy protection was designed to work with. Copying Windows discs under Linux, for example, was a favourite ploy. But the latest DRM technology is burying itself deeper into PCs, making it harder to circumvent.

Intel is now building DRM technologies into processors. Ever since the Pentium D 820/830/840 and the 945 chipset were launched in May 2005, on-chip DRM has been available.

Digital Transmission Content Protection over Internet Protocol (DTCP-IP) is, according to Intel, a standard for secure transmission of protected content between parts of a PC or between devices, such as a computer and a music player. It uses 128-bit encryption to



▲ The Pentium D 840 Extreme Edition has many advantages, but support for Intel's embedded DRM may not be one of them

prevent content being intercepted and copied or tampered with.

Having this kind of encryption built into processors and chipsets, Intel argues, is not DRM as such, but just a conduit for protected content. The rules defining how you can use that content are set out by the content providers, not Intel. But those rules can be draconian. Part of the DTCP-IP standard enables a device to tell a content provider what you're doing with the media you bought. Your DTCP-IP licence could then be revoked, again remotely, making it impossible for you to continue using that device.

Intel's DRM scheme is part of the Trusted Computing platform, which it has been working on with Microsoft, IBM, HP and AMD for several years. Trusted Computing is intended to provide a 'more secure' PC, but part of that security includes the ability for illegitimate software, and the files created by it, to be deleted remotely by the software or content provider.

Trusted Computing has the potential to enable such things as the remote deletion of files on the content providers' terms. It could also prevent you using files created with a rented application if you decide to discontinue rental, perhaps to switch to a rival product. It could also prevent leaks, political or industrial, by refusing to send documents generated within an organisation to a PC outside. It may be that none of these things occur, but the combination of hardware and software within Trusted Computing is a disturbing development.

THE FUTURE

As with so many technologies, DRM can be used for good or bad. While it may be legitimate for content providers to prevent illegal copying or misuse of its content, is it legitimate for them to delete that content or make it unusable on your PC? It's the job of our legal system and the government to decide on remedies for misuse of content, but they also need to regulate Digital Rights Management. In the US, it's already illegal to circumvent any form of DRM under the Digital Millennium Copyright Act, so it's important that DRM is fair in the first place. **CS**



▲ Blu-ray DVDs, which provide up to 30GB of data storage on a single-sided disc, will use two extensions to DRM not found on rival HD DVDs

DRM in the dock The Sony rootkit controversy

Sony, as the main developer of Blu-ray, will have to ensure that the DRM technologies built into the discs work better than XCP did. XCP was the technology Sony BMG applied to over 50 CD titles in 2005, which installed deeply embedded software on any PC on which it was played. The software used 'rootkit' techniques to bury itself deep in a PC's system and live unobserved, and was the subject of several court cases in the US.

Sony has had to offer compensation to disgruntled customers – in the form of

rebates and free music downloads – and has recalled the CDs using XCP. In addition, it has produced routines to uninstall and remove all traces of it from customers' PCs.

This saga highlights the fact that there are controls over what providers can legitimately do to protect their media. It may seem that global companies can impose any restrictions they deem necessary on the media you buy, but they still need to ensure that software they install on your computer doesn't have unintended and potentially harmful effects.